

GRÖBNER BASIS THEORY FOR MODULES OVER POLYNOMIAL RINGS OVER FIELDS WITH VALUATION

ARITRA SEN AND AMBEDKAR DUKKIPATI

ABSTRACT. A motivation to study Gröbner theory for fields with valuations comes from tropical geometry, for example, they can be used to compute tropicalization of varieties (Maclagan & Sturmfels, 2009). The computational aspect of this theory was first studied in (Chen & Maclagan, 2013). In this paper, we generalize this Gröbner basis theory to free modules over polynomial rings over fields with valuation. As the valuation of coefficients is also taken into account while defining the initial term, we do not necessarily get a monomial order. To overcome this problem we have to resort to other techniques like the use of ecart function where the codomain is the well-ordered set \mathbb{N} , and thereby give a method to calculate the Gröbner basis for submodules generated by homogeneous elements. Using this, we show how to compute Hilbert polynomials for graded modules.

1. INTRODUCTION

The Gröbner basis theory of modules has several applications in constructive module theory, for example, in the computation of syzygies, annihilator of a module and Hilbert polynomial of a graded module (Kreuzer & Robbiano, 2005; Spear, 1977; Schreyer, 1986). It has also various applications in homological algebra, for example in the computation of Ext and Tor. In computational algebraic geometry, it is used to compute minimal free resolutions of graded finite modules.

On the other hand, recently Gröbner basis theory for polynomial rings that takes valuation of the underlying field into consideration has been studied by Chan & Maclagan (2013). One motivation for this is its various applications in tropical algebraic geometry. The other motivation comes from computational aspects of Gröbner theory. They can lead to Gröbner bases that are much smaller than the standard Gröbner basis (Remark 4.5). In (Chan & Maclagan, 2013) a normal form algorithm has been presented that leads to an algorithm to compute Gröbner basis in this case. In this paper we generalize this theory to free modules over polynomial rings over fields with valuation.

Contributions. In Gröbner basis theory for modules over polynomial rings over fields with valuation, since the definition of order on monomials involves valuations of coefficients it is not possible to generalize this to the case of modules. So, to overcome this problem we have to resort to other techniques like the use of an ecart function

where the codomain is the well-ordered set \mathbb{N} . Using this, we derive a Buchberger-like criterion for Gröbner basis and hence an algorithm for computing the Gröbner basis. One advantage of this approach is that it can lead to smaller Gröbner basis. With standard Gröbner basis the initial submodule generally grows with degree δ . One particular example where the size of the standard Gröbner basis grows linearly with δ is presented in (Chan & Maclagan, 2013). Here, we give an example of a family of submodules where the size of initial submodules remain constant. Also, with a slight modification, we show how these ideas can be ported to free modules over the polynomial ring $\mathbb{Z}/p^\ell\mathbb{Z}[x_1, \dots, x_n]$.

Organization. The rest of the paper is organized as follows. In Section 2, we present preliminaries on fields with valuation and Gröbner basis over fields with valuation. In Section 3, we introduce free modules over polynomials rings on fields with valuation and a normal form algorithm for them. We present a Buchberger-like criterion for Gröbner basis of submodules using the normal form algorithm of the previous section and then present an algorithm to compute them in Section 4. In Section 5, we show how one can use the algorithm of Section 4 to compute the Hilbert function of a graded module. In Section 6, we introduce free modules over $\mathbb{Z}/p^\ell\mathbb{Z}[x_1, \dots, x_n]$ and present a normal form algorithm for them similar to that of Section 3. A Buchberger-like criterion for Gröbner basis of submodules of modules over $\mathbb{Z}/p^\ell\mathbb{Z}[x_1, \dots, x_n]$ and algorithm to compute the Gröbner basis is presented in Section 6. Finally, we give concluding remarks in Section 7.

2. BACKGROUND

Throughout this paper, K denotes a field and \mathbb{N} the set of natural numbers including zero. For any positive integer n , $[n]$ denotes the set $\{1, \dots, n\}$. A polynomial ring in indeterminates x_1, \dots, x_n over K is denoted by $K[x_1, \dots, x_n]$. For any $\alpha \in \mathbb{N}$ a monomial in indeterminates x_1, \dots, x_n is written as x^α and $|\alpha|$ denotes the sum $\sum_{i=1}^n \alpha_i$. An arbitrary polynomial $f \in K[x_1, \dots, x_n]$ is written as

$$f = \sum_{\alpha \in \Lambda} a_\alpha x^\alpha ,$$

where $a_\alpha \in K$, $\alpha \in \mathbb{Z}_{\geq 0}^n$ and $\Lambda \subseteq \mathbb{Z}_{\geq 0}^n$ a finite set, that is support of the polynomial f , denoted by $\text{supp}(f)$. By monomial we mean x^α , by term we mean $a_\alpha x^\alpha$.

Let S be a finite a set then $|S|$ denotes the number of elements in the set. Let $w = (w_1, \dots, w_n) \in \mathbb{R}^n$ and $u = (u_1, \dots, u_n) \in \mathbb{R}^n$ then $w.u$ represents the sum $\sum_{i=1}^n w_i u_i$. Monomial order on $K[x_1, \dots, x_n]$ is denoted by \prec and for every polynomial $f \in K[x_1, \dots, x_n]$, $\text{in}_\prec(f)$ denotes the initial term with respect to \prec . Let I be an ideal in $K[x_1, \dots, x_n]$, then $\text{in}_\prec(I) = \langle \text{in}_\prec(f) : f \in I \rangle$. \mathbb{Z}_{p^ℓ} represents the finite ring $\mathbb{Z}/p^\ell\mathbb{Z}$.

Definition 2.1. A field with valuation is an ordered pair of a field K and function v , (K, v) such that

- (1) v is a group homomorphism from K^* to $(R, +, 0)$,
- (2) $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in K^*$, and
- (3) $v(a) = \infty$ iff $a = 0$.

The image of the valuation map is denoted by Γ . Let R_K be the set of all field elements with valuation greater or equal to 0, i.e., $R_K = \{c \in K : v(c) \geq 0\}$. Then R is a local ring with maximal ideal $J_K = \{c \in K : v(c) > 0\}$ and $\mathbb{k} = R_K/J$ is the residue field of K . Let $a \in R$, then \bar{a} represents its image in the residue field \mathbb{k} .

Example 2.2. The most common example of a field with valuation is \mathbb{Q} with p -adic valuation $\text{val}_p(\cdot)$, where p is a prime number. Let $q \in \mathbb{Q}$, then $\text{val}_p(q) = c$, where $q = p^c a/b$, such that p does not divide a and b . For example, $\text{val}_3(15/4) = 1$, $\text{val}_2(5/12) = -2$.

Example 2.3. Consider the field of Puiseux series $K\{\{t\}\}$, which is the algebraic closure of the field of Laurent series when $\text{char}(K) = 0$. The map, $\text{val} : K\{\{t\}\} \rightarrow \mathbb{R}$ that takes a Puiseux series and returns the lowest exponent is a valuation. For example, let $f(t) = 3t^{-3} + 6t^{-1} + \dots$ then $\text{val}(f(t)) = -3$.

Definition 2.4. Let $f = \sum_{u \in \Lambda} c_u x^u \in K[x_1, \dots, x_n]$, be a polynomial, where $c_u \in K$, and Λ is the support of f . Let $w \in \Gamma^n$, v be a valuation of K and $W = \min_{u \in \Lambda} \{v(c_u) + w \cdot u\}$. The initial form with respect to w is defined as

$$\text{in}_w(f) = \sum_{v(c_u) + w \cdot u = W} \overline{c_u} t^{-v(c_u)} x^u.$$

Note that in the above definition of W , ‘min’ can be replaced by ‘max’ since for every valuation v and weight vector w one can find a weight vector w' and valuation v' such that both cases coincide.

Example 2.5. Consider the polynomial f over the field of Puiseux series. $f = (1 + t^2)x + 2t^2y + t^3z$. Let $w = (1, 1, 1)$. The initial form of f with respect to w is $\overline{(1 + t^2)}x = x$.

Example 2.6. Consider the polynomial f over \mathbb{Q} with 2-adic valuation, $f = 2x + 5y^2 + 3xyz$. Let $w = (1, 1, 1)$. Then initial form of $\text{in}_w(f) = \bar{1}x + \bar{5}y^2 = x + y^2$.

Given an ideal I in $K[x_1, \dots, x_n]$ and a weight vector $w \in \Gamma^n$, $\text{in}_w(I)$ denotes the ideal $\langle \text{in}_w(f) : f \in I \rangle$. Note that this need not be a monomial ideal.

Example 2.7. Consider the polynomial f in the previous example, $f = 2x + 5y^2 + 3xyz$. Let $w = (1, 1, 1)$. Then initial form of $\text{in}_w(f) = \bar{1}x + \bar{5}y^2 = x + y^2$. Let \prec be the lexicographic ordering, then $\text{in}_{\prec}(\text{in}_w(f)) = x$.

3. NORMAL FORM ALGORITHM FOR MODULES

Let K be a field with valuation and M be free module over $K[x_1, \dots, x_n]$ of rank d . Then $M \cong K[x_1, \dots, x_n]^d$ and hence we work only with $K[x_1, \dots, x_n]^d$.

Every element of the $K[x_1, \dots, x_n]^d$ can be written as

$$\sum_{k=1}^d \sum_{u \in \mathbb{Z}_{\geq 0}^n} c_{u,k} x^u e_k ,$$

where $\{e_1, \dots, e_d\}$ is the standard basis of $K[x_1, \dots, x_n]^d$. In the above representation, $c_{u,k} x^u e_k$ is called a term, $x^u e_k$ is called a monomial and $|u|$ is the degree of the term or monomial. In this case, we define support of $f \in K[x_1, \dots, x_n]^d$, $\text{supp}(f)$, to be the set $\{(u, k) \in \mathbb{Z}_{\geq 0}^n \times [d] : c_{u,k} \neq 0\}$.

Definition 3.1. An element $f \in K[x_1, \dots, x_n]^d$ is called an homogeneous if every monomial occurring in f is of same degree.

Now, we define initial form for the elements of $K[x_1, \dots, x_n]^d$.

Definition 3.2. Let $f = \sum_{(u,k) \in \Lambda} c_{u,k} x^u e_k \in K[x_1, \dots, x_n]^d$, where Λ is the support of f . Let $w \in \Gamma^n$, v be a valuation of K and $W = \min_{(u,k) \in \Lambda} \{v(c_{u,k}) + w \cdot u\}$, where $(u, k) \in \Lambda$. The initial form with respect to w is defined as

$$\text{in}_w(f) = \sum_{\substack{v(c_{u,k}) + w \cdot u = W \\ (u,k) \in \Lambda}} \overline{c_{u,k} t^{-v(c_{u,k})}} x^u e_k.$$

We fix an ordering on the standard bases as $e_1 \prec e_2 \prec \dots \prec e_m$ and \prec be a monomial order. We say that $x^\alpha e_i \prec x^\beta e_j$ if $x^\alpha \prec x^\beta$ or if $x^\alpha = x^\beta$ and $e_i \prec e_j$.

Let $x^u e_k$ be the monomial in $\text{in}_{\prec}(\text{in}_w(f))$. Then $\text{in}_{w, \prec}(f)$ represents the term $c_{u,k} x^u e_k$.

Example 3.3. Let $f = 2x^3 e_1 + 12xy e_2$ and $w = (0, 0)$. Then with 2-adic valuation, $\text{in}_w(f) = x^3 e_1$, $\text{in}_{\prec}(\text{in}_w(f)) = x^3 e_1$ and $\text{in}_{w, \prec}(f) = 2x^3 e_1$.

Now having the definition for initial form of f , we can define the initial submodule for a submodule of $K[x_1, \dots, x_n]^d$.

Definition 3.4. Let I be a submodule of $K[x_1, \dots, x_n]^d$. The initial submodule of I , $\text{in}_w(I)$ is defined as a submodule generated by the initial forms of the elements of I , i.e $\langle \text{in}_w(f) : f \in I \rangle$.

Now we define the Gröbner basis for a submodule

Definition 3.5. Let I be submodule of $K[x_1, \dots, x_n]^d$. A generating set for I , $G = \{g_1, \dots, g_n\}$ is a Gröbner basis for I iff $\text{in}_w(I) = \langle \text{in}_w(g_1), \dots, \text{in}_w(g_n) \rangle$.

Lemma 3.6. *Let I be a submodule of $K[x_1, \dots, x_n]^d$. Let \prec be a monomial order. If $\{g_1, \dots, g_s\}$ is a generating set for I such that $\{\text{in}_w(g_1), \dots, \text{in}_w(g_s)\}$ is a Gröbner basis of $\text{in}_w(I)$ with respect to \prec , then $\{g_1, \dots, g_s\}$ is a Gröbner basis of I with respect to w .*

Proof. Since, $\{\text{in}_w(g_1), \dots, \text{in}_w(g_s)\}$ is a Gröbner basis of $\text{in}_w(I)$, it is also a generating set. Therefore by Definition 3.5, it is a Gröbner basis for I with respect to w . \square

Definition 3.7. Let $c_{\alpha,i}x^\alpha e_i$, $c_{\beta,j}x^\beta e_j$ be terms in $K[x_1, \dots, x_n]^d$, we say $c_\beta x^\beta e_j$ divides $c_\alpha x^\alpha e_i$ if $i = j$ and $c_\beta x^\beta$ divides $c_\alpha x^\alpha$

Now, we are ready to present the division algorithm. For the division algorithm, we will need a notion of ecart function similar to the tangent cone algorithm.

Definition 3.8. Let $f, g \in K[x_1, \dots, x_n]^d$ then $\text{ecart}(f, g) = |\text{supp}(g) - \text{supp}(f)|$.

Theorem 3.9. *Let $f \in K[x_1, \dots, x_n]^d$ be a homogeneous element and $S = \{g_1, \dots, g_s\}$ be a set of homogeneous elements of $K[x_1, \dots, x_n]^d$. Then Algorithm 1 computes r and $h_1, \dots, h_s \in K[x_1, \dots, x_n]$ such that*

$$f = \sum_{i=1}^s h_i g_i + r,$$

where $\text{in}_{w,\prec}(r) \geq \text{in}_{w,\prec}(f)$, $\text{in}_{w,\prec}(h_i g_i) \geq \text{in}_{w,\prec}(f)$ and no monomial of r is divisible by $\text{in}_{w,\prec}(g_i)$ for $i \in \{1, \dots, s\}$.

Proof. Let $q_j, h_{i,j}, r_j$ represent the value of q, h_i, r at the j^{th} iteration. We use induction to prove that following conditions are true for every iteration

- C1:** $f = q_j + \sum_{i=1}^s h_{i,j} g_i + r_j$,
- C2:** $\text{in}_{w,\prec}(h_{i,j} g_i) \geq \text{in}_{w,\prec}(f)$,
- C3:** No term of r_j is divisible by $\text{in}_{w,\prec}(g_i)$, and
- C4:** $\text{in}_{w,\prec}(r_j) \geq \text{in}_{w,\prec}(f)$.

Before the beginning of the while loop, the above conditions are satisfied. The proof then follows by induction.

If there is no $g \in D$ with $\text{in}_{w,\prec}(g)$ dividing $\text{in}_{w,\prec}(q_j)$, then $r_j + q_j = r_{j+1} + q_{j+1}$. Since, the C1 holds true at j^{th} iteration, it is also true for $j+1^{\text{th}}$ iteration. C2 holds true because there is no change in $h_{i,j}$. C3 is true because the new monomial which is being added to r_j is not divisible by $\text{in}_{w,\prec}(g_i)$. C4 is true by the definition of initial form.

Suppose there exists $g \in D$ with $\text{in}_{w,\prec}(g)$ dividing $\text{in}_{w,\prec}(q_j)$ and $g = g_k$ for some $k \in \{1, \dots, s\}$. Since, $q_j + h_{k,j} g_k = q_{j+1} + h_{k,j+1} g_k$, C1 is satisfied. As r_j does not

Algorithm 1 Division algorithm for modules

```

1: Input: A finite set  $B$  of homogeneous elements of  $K[x_1, \dots, x_n]^d$ .
2: Output  $r$  as mentioned Theorem 3.7.
3: Initialize:  $D = \{g_1, \dots, g_s\}$ ,  $h_1 = \dots = h_s = 0$ ,  $q = f$ ,  $r = 0$ 
4: while  $q \neq 0$  do
5:   if there is no  $g \in D$  with  $\text{in}_{w, \prec}(g)$  dividing  $\text{in}_{w, \prec}(q)$  then
6:      $D = D \cup \{q\}$ 
7:      $r = r + \text{in}_{w, \prec}(q)$ ,  $q = q - \text{in}_{w, \prec}(q)$ 
8:   else
9:     Choose  $g \in D$  such that  $\text{in}_{w, \prec}(g)$  divides  $\text{in}_{w, \prec}(q)$  with  $\text{ecart}(g, q)$  minimal.
10:    if  $\text{ecart}(g, q) > 0$  then
11:       $D = D \cup \{q\}$ 
12:       $c = \text{in}_{w, \prec}(q) / \text{in}_{w, \prec}(g)$ .  $l = q - cg$ 
13:      if  $g = g_k$  for some  $k \in \{1, \dots, s\}$  then
14:         $q = l$ 
15:         $h_k = h_k + c$ ,  $h_i = h_i$  for all  $i \neq k$ 
16:         $r = r + cl$ 
17:      else
18:         $q = 1/(1 - c)l$ 
19:         $h_k = 1/(1 - c)(h_k - ch_{k,m})$ 
20:         $r = 1/(1 - c)(r - cr_m)$ 
return  $r$ 

```

change, the C2 and 3 are satisfied. Since $\text{in}_{w, \prec}(q_j) \geq \text{in}_{w, \prec}(f)$ and $\text{in}_{w, \prec}(h_{k,j}g_k) \geq \text{in}_{w, \prec}(f)$, C4 is also satisfied.

Now suppose that the last else statement is executed during the $j + 1^{\text{th}}$ iteration. Note that q_j is a homogeneous element of M and its degree remains same at all iterations. This implies c is a constant term. Consider the the following equations

$$f = q_j + \sum_{i=1}^s h_{i,j}g_i + r_j,$$

and

$$f = q_m + \sum_{i=1}^s h_{i,m}g_i + r_m.$$

Multiplying the second equation by c and then subtracting it from the first equation we see that C1 is satisfied. Now let $\text{in}_{w, \prec}(q_m) = c_m x^\alpha e_k$ and $\text{in}_{w, \prec}(q_j) = c_j x^\alpha e_k$. Since $\text{val}(c_j) + w \cdot \alpha > \text{val}(c_m) + w \cdot \alpha$. We get $\text{val}(c) > 0$, since $c = c_j/c_m$. This implies $\text{val}(1/(1 - c)) = 0$. Since, $\text{val}(c) > 0$ and $\text{val}(1 - c) = 0$, we can see that the C4 is satisfied. Now, since no term of r_j and r_m is divisible by $\text{in}_{w, \prec}(g_i)$, C3 is satisfied.

Now let $s(q_j)$ denote the set of non-zero monomials of $s(q_j)$. Now, since q_j is homogeneous polynomial there are only finitely many values for $s(q_j)$. So by pigeonhole

principle there exists a j such that after j^{th} iteration the values of $s(q_j)$ will be from a fixed set of monomials. So, there will be $j' < j$ such that $s(q_j) = s(q_{j'})$ and therefore $\text{ecart}(q_{j'}, q_j) = 0$. Now, $s(q_{j+1}) \subsetneq s(q_j)$, since the leading term is removed from q_j . So, the algorithm terminates. \square

Example 3.10. Consider $\mathbb{Q}[x, y]^2$ with 2-adic valuation and $w = (1, 1)$ and lex ordering \succ . Let $f = \begin{bmatrix} 5x^3 \\ 7y^3 \end{bmatrix}$ and $g_1 = \begin{bmatrix} 2x^2 \\ 3y^2 \end{bmatrix}$, $g_2 = \begin{bmatrix} 2x \\ 5y \end{bmatrix}$ and $D = \{g_1, g_2\}$. We can write $f = 5x^3e_1 + 7y^3e_2$, $g_1 = 2x^2e_1 + 3y^2e_2$, $g_2 = 2xe_1 + 5ye_2$. Now let us calculate $\text{in}_{w, \prec}(f)$. We have $\text{val}(5) + (1, 1) \cdot (3, 0) = \text{val}(7) + (1, 1) \cdot (0, 3)$. But $x^3 \succ y^3$. We get $\text{in}_{w, \prec}(f) = 5x^3e_1$. Similarly we get $\text{in}_{w, \prec}(g_1) = 2x^2e_1$ and $\text{in}_{w, \prec}(g_2) = 2xe_1$. Let $q_0 = f = 5x^3e_1 + 7y^3e_2$ and $r_0 = 0$. Now $\text{in}_{w, \prec}(g_1)$ divides $\text{in}_{w, \prec}(f)$. So, we get $q_1 = q_0 - 2.5xg_1 = 7y^3e_2 - 7.5xy^2e_2$ and $r_1 = 0$. $D = D \cup \{q_0\}$. Since there exists no $g \in D$ such that $\text{in}_{w, \prec}(g)$ divides $\text{in}_{w, \prec}(q_1)$, we get $q_2 = -7.5xy^2e_2$ and $r = 7y^3e_2$. $D = D \cup \{q_1\}$. Since there exists no $g \in D$ such that $\text{in}_{w, \prec}(g)$ divides $\text{in}_{w, \prec}(q_1)$, we get $q_3 = 0$ and $r_3 = 7y^3e_2 - 7.5xy^2e_2$. Therefore, $r = 7y^3e_2 - 7.5xy^2e_2$.

4. COMPUTATION OF GRÖBNER BASIS FOR SUBMODULES

Definition 4.1. Let $c_\alpha x^\alpha e_i$, $c_\beta x^\beta e_j$ be monomials in $K[x_1, \dots, x_n]^d$. If $i = j$, then we define $\text{LCM}(c_\alpha x^\alpha e_i, c_\beta x^\beta e_j) = \text{LCM}(x^\alpha, x^\beta)e_j$ otherwise LCM is 0.

Similar to S-polynomials, we define S-form for any two elements in $K[x_1, \dots, x_n]^d$.

Definition 4.2. Let f, g be two elements of $K[x_1, \dots, x_n]^d$. Let $x^\alpha e_j = \text{LCM}(\text{in}_{w, \prec}(f), \text{in}_{w, \prec}(g))$. Then S-form of f, g , is given by

$$\text{S-form}(f, g) = \frac{x^\alpha e_j}{\text{in}_{w, \prec}(f)} f - \frac{x^\alpha e_j}{\text{in}_{w, \prec}(g)} g.$$

Theorem 4.3. Let V be an n dimensional vector space over K . Let $v_1, \dots, v_s \in V$ and $c \in K^s$. Consider the polynomial $f_c = \sum_{i=1}^s c_i x_i$ and let $\text{trop}(f_c)$ represents its tropicalization. Then for every v in the subspace generated by v_1, \dots, v_s and $w \in \mathbb{R}^s$, there exists a $c \in K^s$ with $\sum_{i=1}^s c_i v_i = v$ such that the value of function $\text{trop}(f_c)(w)$ is maximized.

Proof. Consider a $c \in K^s$ such that $\sum_{i=1}^s c_i v_i = v$. Assume that v_1, \dots, v_s are linearly dependent, otherwise the proof is trivial. Let $c' \in K^s$ such that $\sum_{i=1}^s c'_i v_i = 0$. Relabel the vectors such that $\text{val}(c'_1) + w_1 = \text{trop}(f_c)(w)$. Now, there exists an λ such that $c_1 = \lambda c'_1$. From this, we get

$$\text{trop}(f_{c-\lambda c'})(w) \geq \text{trop}(f_c)(w)$$

Since, $c - \lambda c'$ has less no zero components than c , we ultimately get b such that $\sum_{i=1}^s b_i v_i = v$ and v_i with non-zero b_i 's are linearly independent. Since, the set $\{v_1, \dots, v_s\}$ can have only finitely many linearly independent subsets, the theorem follows. \square

Now, we state the Buchberger-like criterion for the Gröbner basis of submodules of $K[x_1, \dots, x_n]^d$.

Theorem 4.4. *Let $S = \{g_1, \dots, g_s\} \subset K[x_1, \dots, x_n]^d$ be finite subset and let I be the submodule generated by S in $K[x_1, \dots, x_n]^d$. If the remainder of $\text{S-form}(g_i, g_j)$ on division by S is 0 for all $g_i, g_j \in S$ then S is a Gröbner bases for the submodule I .*

Proof. Suppose $f \in I$. Then f can be written as $\sum_{i=1}^s h_i g_i$, for $g_i \in S$ and $h_i \in K[x_1, \dots, x_n]$ for $i \in \{1, \dots, s\}$. Now, $\text{in}_{w, \prec}(f) \geq \min_{1 \leq i \leq s} (\text{in}_{w, \prec}(h_i g_i))$. Now let $\text{in}_{w, \prec}(f) = c_v x^v e_k$ and $\text{in}_{w, \prec}(h_i g_i) = c_u x^u e_j$. Then we get $\text{val}(c_v) + w \cdot v \geq \min_{1 \leq i \leq s} (\text{val}(c_i) + w \cdot u_i)$. Now using the previous theorem, we choose h_i such that $\min_{1 \leq i \leq s} (\text{in}_{w, \prec}(h_i g_i))$ is maximized and let it be denoted by m . Suppose $\text{in}_{w, \prec}(f) = m$, then we are done. Otherwise, $\text{in}_{w, \prec}(f) > m$. Consider the set $S = \{i : \text{in}_{w, \prec}(h_i g_i) = m\}$. Now $g = \sum_{i \in S} \text{in}_{w, \prec}(h_i) g_i$. But $\text{in}_{w, \prec}(g) < m$, therefore

$$g = \sum_{i, j \in S, i \neq j} c_{i,j} \text{S-form}(x_i g_i, x_j g_j).$$

Now, $x = \text{LCM}(\text{in}_{w, \prec}(x_i g_i), \text{in}_{w, \prec}(x_j g_j))$ So,

$$\begin{aligned} \text{S-form}(x_i g_i, x_j g_j) &= \frac{x}{\text{in}_{w, \prec}(x_i g_i)} x_i g_i - \frac{x}{\text{in}_{w, \prec}(x_j g_j)} x_j g_j \\ &= \frac{x}{x_{ij}} \text{S-form}(g_i, g_j) \end{aligned}$$

where $x_{i,j} = \text{LCM}(\text{in}_{w, \prec}(g_i), \text{in}_{w, \prec}(g_j))$. Since $\text{S-form}(g_i, g_j)$ reduces to 0, it can be written as a sum of g_i, \dots, g_j . Substituting this into g and f , we get a representation of f as $\sum_{i=1}^s h'_i g_i$ but $\min_{1 \leq i \leq s} (\text{in}_{w, \prec}(h'_i g_i)) > m$, a contradiction. \square

The above criterion gives us the following algorithm for computing the Gröbner basis.

Algorithm 2 Algorithm for Gröbner basis for modules

```

1: Input: A finite set  $B$  generating the submodule  $I$  of  $K[x_1, \dots, x_n]^d$ 
2: Output A Gröbner basis for the submodule  $I$ 
3: Initialize  $G = B$ 
4: Initialize  $C = G \times G$ 
5: while  $C \neq \emptyset$  do
6:   Choose a pair  $(f, g)$  from  $C$ 
7:    $C := C - \{(f, g)\}$ 
8:   Divide  $\text{S-form}(f, g)$  by  $G$  using the Algorithm 1. Let the remainder be  $r$ 
9:   if  $r \neq 0$  then
10:     $C := C \cup G \times \{r\}$ 
11:     $G := G \cup \{r\}$ 
return  $G$ 

```

Proof. To prove this, we use the ascending chain condition on the module $K[x_1, \dots, x_n]^d$. Let G_i represent the set G in the algorithm at i^{th} iteration. As the algorithm progresses we get the following strictly increasing set of elements in $K[x_1, \dots, x_n]^d$.

$$G_1 \subsetneq G_2 \subsetneq \dots$$

Let $G_i = G_{i-1} \cup \{r\}$. By Algorithm 1, $\text{in}_{w, \prec}(r)$ is not divisible by the initial form of any of element in G_i . Let $\text{in}_{w, \prec}(G) = \langle \text{in}_{w, \prec}(g) : g \in G \rangle$. Therefore, $\text{in}_{w, \prec}(G_i) \subsetneq \text{in}_{w, \prec}(G_{i+1})$. So, we get an ascending chain of submodules,

$$\text{in}_{w, \prec}(G_1) \subsetneq \text{in}_{w, \prec}(G_2) \dots$$

By noetherian condition, this chain must stabilize at one point. Once the algorithm terminates, $\text{S-form}(f, g)$ for any $f, g \in G$ reduces to zero on division by G . So, by previous theorem it is a Gröbner basis. \square

Remark 4.5. One motivation for studying Gröbner basis for fields with valuation is that they can lead to a smaller Gröbner basis. Consider the module $\mathbb{Q}[x, y, z]^r$, where $r \geq 2$. Consider the submodule $I = \langle f, g, h \rangle$, such that f, g and h are of degree 2ϵ . Every coefficient of f except $x_1^\epsilon x_2^\epsilon e_1$ has positive 2-adic valuation. Every coefficient of g except $x_2^\epsilon x_3^\epsilon e_2$ has positive 2-adic valuation and every coefficient of h except $x_1^\epsilon x_3^\epsilon e_3$ has positive 2-adic valuation. Let $w = (0, 0, 0)$. Then the initial ideal, $\text{in}_w(I) = \langle x_1^\epsilon x_2^\epsilon e_1, x_2^\epsilon x_3^\epsilon e_2, x_1^\epsilon x_3^\epsilon e_3 \rangle$. So, the number of generators of $\text{in}_w(I)$ remains fixed and does not increase with ϵ . Such a bound is not possible with standard Gröbner basis, the number of generators will increase with ϵ . One particular example was shown in (Chan & Maclagan, 2013).

Remark 4.6. Note that the initial ideal $\text{in}_w(I)$ here is dependent on the valuation of the underlying field. So, if the valuation changes $\text{in}_w(I)$ also changes generally. But if $\text{in}_w(I)$ does not contain a monomial and w lies on the unbounded of part of the

tropical variety of I , then $\text{in}_w(I)$ doesn't contain a monomial even if the valuation changes (Fink, 2013).

5. COMPUTATION OF HILBERT POLYNOMIALS

In this section we show how to compute Hilbert polynomials of modules using the theory described in the previous section. The standard strategy for computing Hilbert function is to reduce to the case of monomial ideals. We saw in Remark 4.5 that Gröbner basis in the case of fields with valuation can lead to very small monomial ideals. One can exploit this fact to compute the Hilbert function. In Section 3, our initial submodule was a submodule in the free module over $\mathbb{K}[x_1, \dots, x_n]$. In this section, we take it as a submodule in the free module over $K[x_1, \dots, x_n]$. So, the initial module is a submodule of $K[x_1, \dots, x_n]^d$. Let I be the module of $K[x_1, \dots, x_n]^d$, then let $\text{in}_{w, \prec}(I)$ denotes the submodule $\langle \text{in}_{w, \prec}(f) : f \in I \rangle$ in $K[x_1, \dots, x_n]^d$.

Theorem 5.1. *Let I be a submodule generated by homogeneous elements of $K[x_1, \dots, x_n]^d$. Let B be the set of monomials that do not appear in $\text{in}_{w, \prec}(I)$, then the residue class elements of B form a K -vector space basis for $K[x_1, \dots, x_n]^d/I$.*

Proof. We first show that elements of B are linearly independent. Suppose they are not, then there exists $b_i \in B$, $0 \neq c_i \in K$ such that $f = \sum_{i=1}^n c_i b_i \in I$.

Since $f \in I$, $\text{in}_{w, \prec}(f) \in \text{in}_{w, \prec}(I)$, this implies one of the b_i is in $\text{in}_{w, \prec}(I)$, which is a contradiction.

To show that B spans the vector space, $\{g_1, \dots, g_s\}$ be a Gröbner basis for the submodule I . Let $f + I$ be an element of $K[x_1, \dots, x_n]^d/I$. Let f_δ denote the homogeneous component of f of degree δ . Divide f_δ by g_1, \dots, g_s using the normal form Algorithm 1, let r_δ be the remainder. By the property of the normal form algorithm none of the monomials appearing in r_δ is divisible by $\text{in}_{w, \prec}(g_i)$ for $i \in \{1, \dots, s\}$. Since $\{g_1, \dots, g_s\}$ is a Gröbner basis, this implies all monomials of r_δ belong to B . Since this is true for any δ , $f + I$ can be written as a sum of residue class elements of B . Therefore, they generate $K[x_1, \dots, x_n]^d/I$. \square

Theorem 5.2. *Let $K[x_1, \dots, x_n]^d/I$ be a finitely generated graded module, where I is generated by homogeneous elements. Then the Hilbert function of $K[x_1, \dots, x_n]^d/I$ and $K[x_1, \dots, x_n]^d/\text{in}_{w, \prec}(I)$ are the same.*

Proof. Let B be the set of monomials not in $\text{in}_{w, \prec}(I)$. Let B_δ , I_δ and $K[x_1, \dots, x_n]_\delta^d$ represent the set of elements of degree δ in B , I and $K[x_1, \dots, x_n]^d$. Now,

$$K[x_1, \dots, x_n]^d/I = \bigoplus_{\delta \in \mathbb{N}} K[x_1, \dots, x_n]_\delta^d/I_\delta.$$

By previous theorem, residue class elements of B is a basis for $K[x_1, \dots, x_n]^d/I$, so B_δ forms a basis for $K[x_1, \dots, x_n]_\delta^d/I_\delta$. So, $\dim_k K[x_1, \dots, x_n]_\delta^d/I_\delta = |B_\delta|$. Now, the since $\text{in}_{w, \prec}(\text{in}_{w, \prec}(I)) = \text{in}_{w, \prec}(I)$, the same argument will hold for $K[x_1, \dots, x_n]^d/\text{in}_{w, \prec}(I)$. \square

So, we have reduced the problem of computing the Hilbert polynomial of $K[x_1, \dots, x_n]^d/I$ to the problem of computing the Hilbert polynomial for $K[x_1, \dots, x_n]^d/\text{in}_{w, \prec}(I)$. The Hilbert polynomial of the quotient of a free module by a monomial submodule can computed by standard methods.

6. GRÖBNER BASIS FOR MODULES OVER $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]$

In this section, we extend the above study to free modules over $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]$, where p is a prime and ℓ is a positive integer. Let M be a free module of rank d over $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]$, then $M \cong \mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$. In order to define an ordering on the monomials of $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$, we first define the following map

Definition 6.1. Let $v : \mathbb{Z}_{p^\ell} \rightarrow \{0, 1, \dots, \ell - 1, \infty\}$ be such that if $m = p^k a$ and $\gcd(p, a) = 1$ then $v(m) = k$ and $v(0) = \infty$.

Theorem 6.2. Let $a, b \in \mathbb{Z}_{p^\ell}$ and v is defined as Definition 6.1

- (1) $v(ab) = v(a) + v(b)$ when $ab \neq 0$, and
- (2) $v(a + b) \geq \min\{v(a), v(b)\}$ when $a + b \neq 0$.

Proof. Let $a = p^k c, b = p^{k'} c', \gcd(p, c) = \gcd(p, c') = \gcd(p, cc') = 1$ and $k' + k < \ell$. Now, $ab = p^{k+k'} cc' = qp^\ell + r$. We get $r = p^{k+k'}(cc' - qp^{\ell-k-k'})$. Now, $\gcd(cc' - qp^{\ell-k-k'}, p) = 1$. So, we get $v(ab) = k + k' = v(a) + v(b)$. Now, let $k' < k$. Then $a + b = p^k c + p^{k'} c' = qp^\ell + r$. We get $r = p^{k'} c' + p^k c - qp^\ell = p^{k'}(c' + p^{k-k'} c - qp^{\ell-k'})$. Now, $\gcd(p, c' + p^{k-k'} c - qp^{\ell-k'}) = \gcd(p, c') = 1$. So, $v(a + b) = k'$. \square

Now using the map v from Definition 6.1 we can define ordering on the terms in $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$.

Definition 6.3. Let \succ be a monomial order for $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]$ and let $c_{u,i} x^u e_i$ and $c_{v,j} x^v e_j$ be two monomials. We say that $c_{u,i} x^u e_i \succ c_{v,j} x^v e_j$ if $x^u \succ x^v$ or if $x^u = x^v$ and $e_i \succ e_j$

Definition 6.4. Let w be a weight vector. We say that $c_{u,i} x^u e_i < c_{v,j} x^v e_j$ if $v(c_{u,i}) + w \cdot u < v(c_{v,j}) + w \cdot v$ or $v(c_{u,i}) + w \cdot u = v(c_{v,j}) + w \cdot v$ and $c_{u,i} x^u e_i \succ c_{v,j} x^v e_j$

Definition 6.5. Let $f \in \mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ and $\sum_{k=1}^d \sum_{u \in \mathbb{Z}_{\geq 0}^n} c_{u,k} x^u e_k$, $\text{in}_{w, \prec}(f)$ is $c_{u,i} x^u e_i$, such that $c_{u,j} x^u e_j \leq c_{v,i} x^v e_i$ for all $(v, i) \in \text{supp}(f)$.

Now we define divisibility on terms in $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$.

Definition 6.6. Let $c_\alpha x^\alpha e_i, c_\beta x^\beta e_j$ be monomials in $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$, we say $c_\beta x^\beta e_j$ divides $c_\alpha x^\alpha e_i$ if $i = j$, c_β divides c_α and x^β divides x^α .

In this section, we present a normal form algorithm according to the order given mentioned in Definition 6.4.

Theorem 6.7. Let $f \in \mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ be a homogeneous elements and $S = \{g_1, \dots, g_s\}$ be set of homogeneous elements of $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$. Then Algorithm 1 computes r and $h_1, \dots, h_s \in \mathbb{Z}_{p^\ell}[x_1, \dots, x_n]$ such that

$$f = \sum_{i=1}^s h_i g_i + r,$$

where $\text{in}_{w, \prec}(r) \geq \text{in}_{w, \prec}(f)$, $\text{in}_{w, \prec}(h_i g_i) \geq \text{in}_{w, \prec}(f)$ and no monomial of r is divisible by $\text{in}_{w, \prec}(g_i)$ for $i \in \{1, \dots, s\}$.

Proof. Let $q_j, h_{i,j}, r_j$ represent the value of q, h_i, r at the j^{th} iteration.

The proof is similar to the proof of Theorem 3.9. The difference lies in the third if statement. Assume that j^{th} statement is being executed. Note that q_j is a homogeneous element of $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ and its degree remains same at iteration. Now let $g_j \in D$ be equal to q_m for some m less than j . Note that q_j is a homogeneous element of $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ and its degree remains the same at all iterations. Let $\text{in}_{w, \prec}(q_j) = c_u x^u e_i$ and $\text{in}_{w, \prec}(q_m) = c_v x^v e_i$. Since, degree of q_j and q_m are same we get that $x^u = x^v$. Also, since $\text{in}_{w, \prec}(q_j) < \text{in}_{w, \prec}(q_m)$, we get $\text{val}(c_u) + w \cdot u < \text{val}(c_v) + w \cdot v$. So $\text{val}(-c) > 0$. Therefore, $\gcd(1 - c, p) = \gcd(1 - c, p^\ell) = 1$. This implies $1 - c$ is invertible. The rest of the proof is similar to Theorem 3.9. \square

Example 6.8. Let $M = \mathbb{Z}/8\mathbb{Z}[x, y]^2$ with $w = (1, 1)$ and lex ordering \succ . Let $f = \begin{bmatrix} 4x^3 \\ 6y^3 \end{bmatrix}$ and $g_1 = \begin{bmatrix} 4xy \\ 2y^2 \end{bmatrix}$, $g_2 = \begin{bmatrix} 2x \\ 2y \end{bmatrix}$ and $D = \{g_1, g_2\}$. We can write $f = 4x^3 e_1 + 6y^3 e_2$, $g_1 = 4xy e_1 + 2y^2 e_2$, $g_2 = 2x e_1 + 2y e_2$. Now let us calculate $\text{in}_{w, \prec}(f)$. We have $\text{val}(6) + (1, 1) \cdot (0, 3) < \text{val}(4) + (1, 1) \cdot (3, 0)$. We get $\text{in}_{w, \prec}(f) = 6y^3 e_2$. Similarly, we get $\text{in}_{w, \prec}(g_1) = 4xy e_1$ and $\text{in}_{w, \prec}(g_2) = 2x e_1$. Let $q_0 = 4x^3 e_1 + 6y^3 e_2$ and $r_0 = 0$. Since there exists no $g \in D$ such that $\text{in}_{w, \prec}(g)$ divides $\text{in}_{w, \prec}(q_1)$, we get $q_1 = 4x^3 e_1$, $r_1 = 6y^3 e_2$ and $D = D \cup \{q_0\}$. Now $\text{in}_{w, \prec}(g_2)$ divides $\text{in}_{w, \prec}(q_1)$. So, we get $q_2 = q_1 - 2x^2 g_2 = -4x^2 y e_2$, $r_2 = 6y^3$ and $D = D \cup \{q_1\}$. Since there exists no $g \in D$ such that $\text{in}_{w, \prec}(g)$ divides $\text{in}_{w, \prec}(q_2)$, we get $q_3 = 0$ and $r_1 = 6y^3 e_2 + 4x^2 y e_2$. Therefore, we get $r = 6y^3 e_2 + 4x^2 y e_2$.

Definition 6.9. Let $c_\alpha x^\alpha e_i, c_\beta x^\beta e_j$ be monomials in $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$. If $i = j$, then $\text{LCM}(c_\alpha x^\alpha e_i, c_\beta x^\beta e_j) = \text{LCM}(c_\alpha, c_\beta)(\text{LCM}(x^\alpha, x^\beta))e_j$ otherwise is 0.

We define S-form of two elements of $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ which is similarly to the definition 4.2.

Following is the Buchberger-like criterion for Gröbner basis in this case

Theorem 6.10. *Let $S \subset \mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ be a finite subset and let I be the submodule generated by S in $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$. If the remainder of $S\text{-form}(g_i, g_j)$ on division by S is 0 for all $g_i, g_j \in S$ then S is a Gröbner bases for the submodule I .*

Proof. The proof is similar to Theorem 6.4. The maximum of $\min(\text{in}_{w, \prec}(h_i g_i))$ is guaranteed because there are only finitely many ways to write f as a sum of g_i as \mathbb{Z}_{p^ℓ} is finite. \square

The algorithm for computing the Gröbner basis is the same as Algorithm 2. Here we present the proof of correctness.

Proof. Since \mathbb{Z}_{p^ℓ} is a finite ring therefore it is noetherian. Now using Hilbert basis theorem we get $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]$ is noetherian. Since, $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ is finitely generated, $\mathbb{Z}_{p^\ell}[x_1, \dots, x_n]^d$ is a noetherian module. Rest of the goes along the same line as the proof of Algorithm 2. \square

7. CONCLUSION

In this paper, we studied a generalization of Gröbner basis for modules that also takes the valuation of coefficients into account. We expect the algorithms presented in this paper to have many computational advantages. For example, they can lead to smaller Gröbner basis. Also, to deal with blowing up of coefficients one can first compute the Gröbner basis over \mathbb{Z}_{p^ℓ} and then lift it to the field \mathbb{Q} .

REFERENCES

- BACHMANN, O., GREUEL, G.-M., LOSSEN, C., PFISTER, G. & SCHÖNEMANN, H. (2007). *A Singular introduction to commutative algebra*. Springer.
- CHAN, A. J. & MACLAGAN, D. (2013). Groebner bases over fields with valuations. *arXiv preprint arXiv:1303.0729*.
- COX, D. A., LITTLE, J. & OSHEA, D. (2007). *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer.
- FINK, A. (2013). Tropical cycles and chow polytopes. *Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry* **54**(1), 13–40.
- KREUZER, M. & ROBBIANO, L. (2005). *Computational commutative algebra*, vol. 1. Springer.
- MACLAGAN, D. & STURMFELS, B. (2009). Introduction to tropical geometry. *Book in preparation*.
- MORA, T., PFISTER, G. & TRAVERSO, C. (1992). An introduction to the tangent cone algorithm. vol. 6. pp. 199–270.

- SCHREYER, F.-O. (1986). Syzygies of canonical curves and special linear series. *Mathematische Annalen* **275**(1), 105–137.
- SPEAR, D. A. (1977). A constructive approach to commutative ring theory. *Proc. of the 1977 MACSYMA Users' Conf.* , 369–376.
- WINKLER, F. (1988). A p -adic approach to the computation of gröbner bases. *Journal of Symbolic Computation* **6**(2), 287–304.
- E-mail address:* `a.sen@csa.iisc.ernet.in`, `ad@csa.iisc.ernet.in`

DEPT. OF COMPUTER SCIENCE & AUTOMATION, INDIAN INSTITUTE OF SCIENCE, BANGALORE
- 560012